UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/716,221	11/21/2000	Hisashi Inoue	2000 1451A	9406

7590 06/28/2005

Wenderoth Lind & Ponack LLP
2033 K Street NW
Suite 800
Washington, DC 20006

EXAMINER	
PARTHASARATHY, PRAMILA	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 06/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No. 09/716,221	Applicant(s) INOUE ET AL.
	Examiner Pramila Parthasarathy	Art Unit 2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *5/4/2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 - 19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,7,9,10,13,15,16 and 19* is/are rejected.

7)☒ Claim(s) *2,5,6,8,11,12,14,17 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

Original application contained Claims 1 – 18. Applicant added Claim 19. Therefore, presently pending claims are 1 – 19.

2. Applicant's submission filed on May 04, 2005 has been entered and made of record.

Response to Remarks/Arguments

3. Remarks mistakenly read, Claim 14 to depend on Claim 8 (see Remarks Page 24 line 8). Examiner reads Claim 14 to depend on Claim 13.

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 1, 3, 7, 9, 13,15 and 19 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1 - 48 of Katsura et al. (U.S. Patent No. 6,639,997, hereafter "Katsura").

As per Claims 1,3,7,9,13, 15 and 19 of instant application, Claims 1, 17 and 33 of Katsura similarly recites a digital information embedding/extracting apparatus comprising band division means for dividing said digital image signal into coefficients in a plurality of frequency bands, information embedding means for embedding pseudo-random number string structured by the coefficients in every or some of said divided frequency bands exclusive of a lowest frequency band referred to as MRA (hereinafter,

referred to as MRR), band synthesis means for reconstructing the digital image signal in which said pseudo-random number string has been embedded by using said MRR and MRA to which information embedding processing is subjected. Instant claims further recite "an authentication data generation portion operable to generate a pseudo-ransom number series by using predetermined key data, and to generate authentication data from the pseudo-random number series; an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency band exclusive of the MRA among the plurality of frequency bands". Embedding authentication data in the frequency band is well known in the art (admitted prior art), which provides proof for digital data tampering. Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized that an authenticating data embedding step with a digital information embedding/extracting apparatus of a type embedding inherent digital information in a digital image signal would provide a tamper detection and proof of copy protection.

5. Applicant's remarks/arguments filed on April 13, 2005, with respect to Claims 1, 3, 4, 7, 9, 10,13,15, 16 and 19, have been fully considered but they are not persuasive.

Referring to the previous Office action, Examiner had cited relevant portions of the references as a means to illustrate the system as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims.

6. Applicant agrees that Nakamura disclose an apparatus for embedding watermark information in image data and generates random number for respective bits of watermark information, embedding watermark information in coefficients of a low frequency domain and authentication data. Applicant also agrees that Nakamura divides an entire image into blocks and then performs a band division process, see remarks Page 25 lines 11 – 15.

7. Regarding independent Claims 1, 3, 7, 9, 13,15 and 19, applicant argued that Nakamura et al. U.S. Patent Number 6,185,312, hereafter "Nakamura" and Barton 6,047,374, hereafter "Barton", do not disclose or suggest that "a key data is embedded in transform coefficients of a lowest frequency band (i.e., MRA) among a plurality of frequency bands", "authentication data embedding portion operable to embed authentication data in transform coefficients of frequency bands exclusively of the MRA among the plurality of frequency bands". These arguments are not persuasive.

8. Nakamura's method of embedding digital image by embedding authentication information when combined with Barton's method for generating, embedding and extracting authentication information of a digital block (Barton Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28), provides a key data embedded in transform coefficients of a lowest frequency band (Nakamura Column 6 lines 4 – 57) and an authentication (a second type of data) embedded in transform coefficients of the frequency bands (Column 8 line 31 – Column 17 line 46). Nakamura further discloses

an (entire) image as input where a band division portion operable to divide the digital image signal of the image into a plurality of frequency bands (Column 41 lines 22 – 27).

9. Examiner respectfully asserts that cited prior art does teach or suggest the subject matter broadly recited in independent claims 1, 3, 7, 9, 13,15, 16 and 19. Dependent claims 4, 10 and 16 are also rejected at least by virtue of their dependency on independent claims and by other reason set forth in this office action.

Accordingly, the rejection for the pending Claims 1, 3, 4, 7, 9, 10,13,15, 16 and 19 is respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 1, 3, 4, 7, 9, 10,13,15, 16 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakamura et al. (U.S. Patent No. 6,185,312) in view of Barton (U.S. Patent No. 6,047,374 hereinafter "Barton").

Regarding Claim 1, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and generate authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

a key data embedding portion operable to embed the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 #22, 23 and Column 6 lines 4 – 57);

an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46); and

a band synthesis portion operable to reconstruct the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 3, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the tamper detecting apparatus comprising:

a band division portion operable to divide the digital image signal into a plurality of frequency bands (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43);

a key data extraction portion operable to extract key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for

extracting the key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and to generate authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

an embedded information extraction portion operable to extract embedded information embedded based on the key data by the specific apparatus from transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Barton Fig. 2 # 42, Column 4 lines 22 – 41 and Column 7 line 55 – Column 8 line 28); and

a tamper determination portion operable to compare the embedded information with the authentication data for verification and to determine whether the digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate, embed and extract the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding and extracting digital image with authentication information. The motivation would have been to provide security against

unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 7, Nakamura teaches and describes a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), said method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 # 11 and Column 5 lines 42 – 44);

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 #31 and Column 5 lines 42 – 55);

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 and Column 6 lines 4 – 57);

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 9, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose extracting key data extraction means for extracting the key

data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28),

generating a pseudo-random number series by using the key data, and generating authentication data from the pseudo-random number series (Fig. 3 #31 and Column 5 lines 42 – 55);

extracting embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28);

comparing the embedded formation with the authentication data for verification and determining whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information.

The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 13, Nakamura teaches and describes a recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper-detection-information embedding method of embedding predetermined information for tamper detection in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), computer device readable instruction including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 44);

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

embedding the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46);

embedding the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 and Column 17 line 46); and

reconstructing the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 15, Nakamura teaches and describes a recording medium on which a program having computer device readable instructions to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), computer

device readable instructions including instructions capable of instructing a computer device to perform the method comprising:

dividing the digital image signal into a plurality of frequency bands (Fig. 2 #11 and Column 5 lines 42 – 55);

extracting key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands;

generating a pseudo-random number series by using predetermined key data, and generating authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 # 22, 23 and Column 6 lines 4 – 57). Nakamura does not explicitly disclose key data extraction means for extracting the key data embedded by the specific apparatus from transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands. However Barton discloses a method and apparatus for generating, embedding and extracting authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28), and

comparing the embedded information with the authentication data for verification and determining whether the digital image has been tampered with (Barton Fig. 2, Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing tamper proof authentication information and to provide secure and reliable digital information.

Regarding Claim 19, Nakamura teaches and describes a tamper-detection-information embedding apparatus for embedding predetermined information for tamper detection in a digital image signal, (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), the apparatus comprising:

a band division portion operable to divide the digital image signal of an entire image on which no block division is performed into a plurality of frequency bands (Fig. 2 #11, Column 5 lines 42 – 44 and Column 41 lines 22 – 27);

an authentication data generation portion operable to generate a pseudo-random number series by using predetermined key data, and generate authentication data from the pseudo-random number series (Fig. 3 # 31 and Column 5 lines 42 – 55);

a key data embedding portion operable to embed the key data in transform coefficients of a lowest frequency band (hereinafter, referred to as MRA) among the plurality of frequency bands (Fig. 3 #22, 23 and Column 6 lines 4 – 57);

an authentication data embedding portion operable to embed the authentication data in transform coefficients of the frequency bands exclusive of the MRA (hereinafter, referred to as MRR) among the plurality of frequency bands (Fig. 6 – 10 and Column 8 line 31 – Column 17 line 46); and

a band synthesis portion operable to reconstruct the digital image signal in which the information has been embedded by using the MRA and the MRR to which data embedding processing is subjected (Fig. 2, 6 – 12; Column 8 line 45 – Column 11 line 16, Column 15 line 25 – Column 18 line 57 and Fig. 51 – 54, Column 38 line 42 – Column 39 line 25).

Nakamura does not explicitly teach generating authentication data from the pseudo-random number series. However, Barton discloses a method and apparatus for generating and embedding authentication information of a digital block (Barton Fig. 2, Column 4 lines 22 – 41 and Column 7 line 55 – Column line 28). Therefore it would have been obvious to one of ordinary skill in the art at the time the invention was made to generate and embed the authentication information as taught by Barton, in transform coefficients of the frequency bands as taught by Nakamura to provide a method of embedding digital image by embedding authentication information. The motivation would have been to provide security against unauthorized use or copying by providing

tamper proof authentication information and to provide secure and reliable digital information.

Claim 4 is rejected as applied above in rejecting claim 3. Furthermore, Nakamura teaches and describes a tamper detection apparatus for detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein said tamper determination portion comprises:

a block division portion operable to divide the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

a regional embedded information read portion operable to read, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information extracted by the embedded information extraction portion (Fig. 10, Column 16 lines 17 – 37);

a regional authentication data read portion operable to read, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read by the regional embedded information read means, serially from all of the authentication data generated by the authentication data generation portion (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

a block-tamper determination portion operable to compare the embedded information serially read with the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 10 is rejected as applied above in rejecting claim 9. Furthermore, Nakamura teaches and describes a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), further comprising

dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information (Fig. 10, Column 16 lines 17 – 37);

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

comparing a series of the embedded formation serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim 16 is rejected as applied above in rejecting claim 15. Furthermore, Nakamura teaches and describes a recording medium on which a program to be run on a computer device is recorded for carrying out a tamper detecting method of detecting tamper with a digital image based on tamper-detection-information embedded by a specific apparatus in a digital image signal (Fig. 1 – 4 and Column 5 line 21 – Column 6 line 43), wherein the computer device to perform the method further comprising:

dividing the digital image into a plurality of unit blocks each composed on a predetermined number of pixels (Fig. 2 # 11, Column 5 lines 42 – 44; Fig. 9, Column 14 line 61 – Column 15 line 55, Fig. 12, 13, Column 17 lines 21 – 32 and Fig. 25, 26, Column 23 lines 15 – 46);

reading, for each of the unit blocks, embedded information embedded in the transform coefficients of the MRR that represents the same spatial region as the unit block, serially from all of the embedded information (Fig. 10, Column 16 lines 17 – 37);

reading, for each of the unit blocks, authentication data corresponding in position to the embedded information serially read, serially from all of the authentication data (Fig. 10, Column 16 lines 17 – 53 and Fig. 35 Column 28 line 5 – Column 29 line 41); and

comparing a series of the embedded formation serially read with a series of the authentication data serially read and determining, for each of the unit blocks, whether the digital image has been tampered with (Barton Fig. 2 Column 1 line 65 – Column 2 line 18 and Column 7 line 55 – Column 8 line 28).

Claim Objections

11. Claims 2,5,6,8,11,12,14,17 and 18 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

13. Examiner's Note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested from the applicant, in preparing the

responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO Form 892.

Applicant is urged to consider the references. However, the references should be evaluated by what they suggest to one versed in the art, rather than by their specific disclosure. If applicants are aware of any better prior art than those are cited, they are required to bring the prior art to the attention of the examiner.

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Pramila Parthasarathy whose telephone number is 571-272-3866. The examiner can normally be reached on 8:00a.m. To 5:00p.m.. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-232-3795. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR only. For more information about the PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Pramila Parthasarathy
June 22, 2005.

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100